
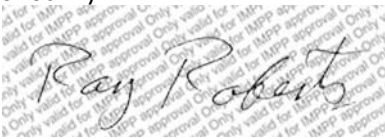


KANSAS DEPARTMENT OF CORRECTIONS

	INTERNAL MANAGEMENT POLICY AND PROCEDURE	SECTION NUMBER	PAGE NUMBER
		05-121	1 of 12
		SUBJECT: INFORMATION TECHNOLOGY AND RECORDS: Network Usage and Management	
Approved By:  Secretary of Corrections		Original Date Issued:	01-21-97
		Replaces Version Issued:	06-26-06
		CURRENT VERSION EFFECTIVE:	08-07-14

POLICY STATEMENT

The Division of Information Services and Communication (DISC) manages the Kansas State Network through the use of dedicated data circuits (KanWin) located throughout the state at all state agencies. The network infrastructure is a critical communications system for the Department of Corrections. The data network is necessary to manage applications, connecting and sharing information with other agencies, and improving interactions with other entities. Individual units in the department may own network hardware and applications that are compliant with defined standards/products defined by the State in compliance with KSA 75-4709.

All network related acquisitions and services provided to the department or any subordinate unit shall be procured to benefit the department as a whole. All network devices, communications lines and network protocols shall be managed at all times. Information technology network technicians play important roles in the design, development, deployment and accountability of all devices and services provided under their span of control. Network architecture must consider centralized management of resources while permitting distributed allocation of the devices and responsibilities. Acquisition of systems must consider the organizational objectives in addition to the economic value of the access, service, performance and availability of the components. All networks must be compliant with state network architecture to include provisions for user access to authorized systems from anywhere in the state.

Information dissemination may take several forms. These include voice, data, video, multimedia and other digital formats. The administration of these is necessary to ensure long-term support, maintenance and compatibility with other agencies.

Cellular telephones and pagers are only to be used for official business. Cellular phones are not to be used from employees' office unless there is a valid reason to do so (phone busy with another call, phone line out of service, etc.) In the event it is necessary to use a cellular phone for personal use, the employee will reimburse the agency for the cost of those calls. Detailed bills listing cellular phone calls are received by each business office. These bills shall be reviewed by the user and any personal calls shall be noted so the amount of any reimbursement can be determined.

DEFINITIONS

D.I.S.C.: The Division of Information Services and Communication

Enterprise Security Officer: A person appointed/designated by the Chief Information Officer (CIO) who is responsible for the operation and security of a network.

Fire Wall: A software or hardware system which prevents or restricts the unauthorized access to or from a network.

Frame Relay Circuit: A special telephone line with available circuit speeds from 56 KB through a T1, used for data/voice/video transmissions.

Local Area Network (LAN): A communications network that serves users within a confined geographical area. It is made up of servers, workstations, a network operating system and a communications link.

Network: An internal or external series of devices physically and/or logically connected together to exchange information.

MAC Address: The unique serial number burned into Network Interface Cards that identifies that network card from all others.

Owner: Agency or other organizational entity that has responsibility for making communication judgments and decisions on behalf of the State with regards to identification, risk classification, value, and protection of the State's IT resources, or portion thereof.

PDA: (**P**ersonal **D**igital **A**ssistant) A handheld computer that serves as an organizer for personal information. It generally includes at least a name and address database, to-do list and note taker. PDAs are pen based and use a stylus to tap selections on menus and to enter printed characters. Data is synchronized between the PDA and desktop computer via cable or wireless transmission.

Router: A device that forwards data packets from one local area network (LAN) or wide area network (WAN) to another. Based on routing tables and routing protocols, routers read the network address in each transmitted frame and make a decision on how to send it based on the most expedient route (traffic load, line costs, speed, bad lines, etc.).

Supplier of Service: Organizational unit that provides IT services to others or to itself in support of the State's mission and goals.

Unauthorized Use/Access: Willfully, fraudulently and without authorization gaining or attempting to gain access to any computer, computer system, computer network or to any computer software, program, documentation, data or property contained in any computer, computer system or computer network.

User: Individual or organizational unit that is authorized to use IT resources.

Video Conferencing Coordinator(s): Kansas Department of Corrections staff of the Central Office and facility/parole region that are responsible for the operation of on-site video equipment and/or scheduling of the equipment/room for video conferencing.

Wide Area Network (WAN): A communications network that covers a wide geographic area, such as state or country. A LAN (local area network) is contained within a building or complex, and a MAN (metropolitan area network) generally covers a city or suburb.

PROCEDURES

I. Network Connections

A. Responsibilities:

1. The Information Technology CIO:
 - a. Shall be responsible for determining and/or approving the need and speed of a circuit based on the facility needs.
 - b. Design and maintain a network that is fault tolerant with a high level of recoverability and moderate level of redundancy.
 - c. Maintain a database of all authorized users to the network.
2. The Enterprise Security Officer shall be responsible for ordering circuits through DISC.

- a. The ESO shall prepare all necessary forms for submission to DISC, which contain all pertinent information regarding the connection.
 - b. The ESO shall maintain logs detailing all information for the connection (i.e., circuit number, location, speed, number of users, etc).
 - c. The ESO shall act as liaison between the facilities/offices and DISC or any other vendor in the connection to a network. Any deviance from this policy shall be approved by the Enterprise Security Officer.
 - d. Internal wiring or connection to the circuit shall be the responsibility of the requesting location.
 - e. Any deviation from standard network connections shall be submitted to the Enterprise Security Officer for approval 60 days prior to the date the location requires connection/service. This shall include, but is not be limited to:
 - (1) Integrated Service Digital Network (ISDN);
 - (2) Digital Subscriber Line (DSL);
 - (3) Asymmetric Digital Subscriber Line (ADSL);
 - (4) Wireless Local Area Network (WLAN)
 - (5) Cable Modem, and/or
 - (6) Desktop video.
 - f. All requests for circuits and systems connected to the network must meet standards addressed in Kansas Statewide Technical Architecture.
 - g. Shall prepare monthly reports regarding communication costs for budgetary controls.
 - h. Enforce acceptable use policies and report violations to the CIO.
 - (1) The CIO may elect to notify the supervisor or individual's appointing authority of violations.
3. Network Technicians:
- a. Develop, update and maintain wiring plans that are compliant with Kansas Statewide Technical Architecture standards.
 - b. When installing new wiring or replacement wiring, install the most recent cable standards.
 - c. Install pathways (conduits, cable trays, etc.) for new wiring.
 - d. Install single mode fiber over multimode fiber.
 - (1) Match new fiber optic cable (50 μ) with older fiber optic cable (62.5 μ).
 - (2) Install single mode fiber when video conferencing or high bandwidth applications are being considered for the network.

- (3) Any requests to install new multimode fiber must be approved by the ESO prior to the purchase or installation of the fiber cable.
- e. Clearly label all cables and network device ports.
- f. Institute recovery procedures that will ensure resumption to full service within an appropriate time frame which may depend on external sources for the outage. Progress on the status of the outage shall be communicated to the location appointing authority as well as the CIO.
 - (1) Two hours during normal duty hours
 - (2) Twelve hours during non-office hours.
- g. Ensure that hardware managing sensitive information is protected with local firewalls.
 - (1) Small office firewalls may utilized firewall software as approved by Enterprise Security Officer.
- h. Maintain spare hardware sufficient to replace network devices and to replace at least 10% of computers.
- i. Maintain a complete and accurate blueprint showing all cable locations with color coding to specify which type of cable it is.

II. Data Network Administration

A. Requests For Electronic Network Access

- 1. Anyone needing access to the Electronic Network shall request approval from the ESO
 - a. The User Network and Communications Awareness Statement, Form #05-172-001 shall be completed and signed by new employees at hire.
 - b. Current employees, contract personnel, and volunteers having access to the Electronic Network shall execute an Information Technology Services Access Agreement, Form 05-145-001.
- 2. The memorandum shall be signed and approved by the Warden, Parole Director, Community Corrections Director, or Central Office division head prior to forwarding to the ESO
- 3. The ESO is responsible to maintain a database of all network users

III. Voice Network Administration:

A. Requests for Voice Services

- 1. The local business unit's telecommunications coordinators shall develop the procedures for the acquisition, installation and maintenance of telephone service.
- 2. Conference Calling Cards:
 - a. The Department of Corrections Telecommunications Manager shall process all requests for conference calling cards in accordance with policies detailed in DISC Policy and Procedure Memorandum 5214.

- (1) All employees with conference calling cards must notify the department's Telecommunications Manager when the need for the calling card no longer exists.
3. All requests for new or upgrade of voice systems must be made in writing to the CIO IMPP form (request for Information Technology Service or Equipment)
 - a. All requests shall be forwarded by the CIO to the DISC representative for review and approval.
- B. Responsibilities:
 1. CIO
 - a. Approve the acquisition of Private Branch Exchanges and contracts for long term telephone services.
 - b. Review all requests with the Central Office Telecommunications Manager for compliance with DISC and departmental requirements.
 2. Local Business Units:
 - a. Ensure that Direct Inward System Access (DISA) to Private Branch Exchanges are disabled to prevent fraud.
 - b. Contact the Department Telecommunications Manager concerning any incidences of fraud or lost calling (KANS-A-N) cards.
 - c. Restrict access to telephone communications rooms and maintain a roster of those persons who access the telephone room. The roster must:
 - (1) Be posted near the entrance of the room or maintained by the campus key control custodian.
 - (2) List staff by name who have unescorted access
 - (3) Identify personnel who are allowed escorted access
 - (4) Identify personnel who are not authorized access under any circumstances.
 - (5) Maintain logs of persons who access the telecommunications room.
 - (6) Communication equipment room shall be labeled with sign "Authorized Personnel Only"
 - (a) The key shall be controlled by the facility/office control center.
 - (b) A log shall be maintained listing who and why the room is entered.
 - d. Program local PBXs to restrict overseas phone calls and locations serviced by the "809" or other inappropriate area codes (such as 900, 976, and "976 look-alikes").
 - e. Block access to 1010XXX+1 numbers that will allow callers to use a long distance carrier of their choice and bill the call to the telephone line.

- f. Disable maintenance ports or modem lines that provide remote access to the PBX, key system or voice mail system.
- 3. Telecommunications Manager:
 - a. Report voice fraud to Department of Information Systems and Communications.
 - b. Investigate all instances of potential fraud or misuse as requested by the DISC Calling Card Administrator.
- B. Staff:
 - 1. Do not transfer outside parties to other lines.
 - 2. Report any of the below possible fraud incidences to the Telecommunications Manager:
 - a. Callers representing themselves as “telephone company repair” or other organization requesting a transfer to an outside line.
 - b. Callers requesting to be transferred to non existent stations beginning with 9 and 1 followed by three digits. This technique might enable the caller to complete the dialing to a long distance site.
 - 3. Replace the default passwords on voice mailboxes with unique passwords.

III. Wireless Communications Administration

- A. Standards: Wireless networks must adhere to the below standards.
 - 1. Must Support 128 bit encryption.
 - 2. Network assignment must be at the Media Access Control (MAC) Address level.
 - 3. PDAs must be protected at the operating system level.
- B. Requests for Wireless Communications Services:
 - 1. Each facility and office must establish procedures for the acquisition of wireless communications to include cellular phones.
 - 2. Installation of mobile data terminals must be approved by the ESO.
 - 3. Utilization of a personal digital assistant (PDA) or flash drive must be approved by the ESO or designee.
 - 4. Personally owned PDAs shall not be allowed access to any wireless network.
 - 5. Facilities/offices may furnish PDA's and/or flash drives to selected staff. Users shall read and sign Attachment B of this IMPP prior to being allowed use of these devices.
 - 6. Cellular Phone Usage:
 - a. Cellular phones will be issued to staff to improve customer service and enhance departmental business and is not considered a personal benefit.

Users shall be required to read and sign Attachment A of this IMPP prior to the use of cellular phones.

- b. The Department will seek reimbursement for costs incurred by the department for personal calls that creates an additional charge to the department.
- c. Each supervisor of staff who utilizes a cellular phone must review and sign monthly activity statements for subordinate staff members. The review will do the following:
 - (1) Determine that the phone is being used for official purposes.
 - (2) Check for the accuracy of the bill.
 - (3) Report to the local business manager charges that exceed the plan's maximum minutes or base rate due to personal calls.
- d. Staff who use personally owned cellular phones while operating a moving state owned vehicle or operating potentially hazardous equipment will be held personally and financially responsible for all damages resulting from the use of the personal cellular phone.
- e. Violation of this policy may result in disciplinary action in accordance with provisions of KSA 75-2949.

C. Responsibilities

- 1. ESO
 - a. Review and approve installation of mobile data terminals to ensure compliance with existing wireless security policies and regulations.
 - b. Report any abuse, fraud or misuse of wireless telecommunications services to the CIO
- 2. Local Business Units:
 - a. Acquire wireless communication services in accordance with state procurement regulations.
 - b. Conduct monthly review of wireless communications utilization to ensure that usage is limited to official business purposes.

IV. Inmate Telephones

A. Requests for Inmate Telephone Services:

- 1. The Kansas Department of Corrections Central Office shall be responsible for the coordination for the installation, maintenance and monitoring of Inmate Telephone Services at all KDOC sites.
- 1. All requests for additions, deletions or modifications to any existing Inmate Telephones, shall be directed to the Kansas Department of Corrections Telecommunications Manager.
- 2. The Kansas Department of Corrections Telecommunications Manager shall direct all work to the Inmate Telephone Prime Contractor for completion of requested work.

B. Responsibilities:

1. Deputy Secretary Facility Management
 - a. Manage the execution of inmate telephone contracts.
 - b. Develop and publish the Request for Proposals for inmate telephone services.
 - c. Review all request as necessary with the Telecommunications Manager.
2. Wardens:
 - a. Publish policies and procedures on the utilization of inmate phones.
 - b. Local units shall designate a staff member to be the Point of Contact between the facility and the Kansas Department of Corrections Telecommunications Manager for coordination of all service for the Inmate Telephone System
 - c. Contact the Kansas Department of Corrections Telecommunications Manager on issues relating to the following:
 - (1) Fraud, misuse or wrongful appropriation of services
 - (2) Vendor support
 - (3) Communication line services
 - (4) Public complaints
3. Telecommunications Manager; Corrections Manager Facility management
 - a. Shall maintain all necessary contact with the Prime Contractor regarding any and all requirements necessary to manage the Inmate Telephone System.
 - b. Resolve vendor issues relating to the following:
 - (1) Fraud, misuse or wrongful appropriation of services
 - (2) Vendor support
 - (3) Communication line services
 - (4) Public complaints
 - (5) Billing and payments to Kansas Department of Corrections an facilities

V. Video Conferencing

A. Requests for Video Conferencing Services

1. All requests for the acquisition of video conferencing components and external services must be approved by the CIO

2. Acquisition of video conferencing components must conform to prevailing state standards as defined in the Kansas State Technical Architecture.
3. Equipment shall be purchased from existing state contracts unless otherwise approved by the CIO

B. Scheduling Coordination and Charges for Service

1. Point-to-Point video conferencing within a facility or campus requires scheduling between the parties involved. These services must be for official purposes.
2. Multi-Point video conferencing sessions will be coordinated with procedures established for the specific system. The Kansas Department of Corrections Video Conferencing Coordinator should be notified of these sessions.
3. Video Conferencing sessions using the Wide-Area Network must be coordinated with the Kansas Department of Corrections Video Conferencing Coordinator.
 - a. Kansas Parole Board video conferencing use shall be scheduled three (3) months in advance.
 - b. Any location desiring to use video conferencing shall send a completed Video Conference Request form (Attachment C, Form #05-121-03) with all required information and authorization(s) to the Kansas Department of Corrections Video Conference coordinator.
 - c. When practical, requests for planned use of multi-point video conferencing shall be received in the Central Office at least one (1) week prior to the scheduled use of the equipment.
 - d. Non-KDOC agency requests for video conferencing request shall be submitted at least two (2) weeks in advance, per procedures in Section V.
 - e. Emergency requests shall be processed based on the nature and type of confirmed emergency.
4. Network based video conference normally does not involve user cost or fees. Costs of the hardware and connectivity services will be the responsibility of the party requesting the video conference service.
5. Network connections for any video-conference shall be established thirty (30) minutes prior to the requested conference time for multi-point conferences and fifteen (15) minutes prior to the requested start time for point-to-point conferences.

C. Video conferencing sites shall be available during the hours of 7:00 a.m. and 5:00 p.m., excluding State observed holidays.

D. Video Recording

1. The Video Conferencing Coordinator at any location wishing to record a video conference shall, at the beginning of the conference, announce to all locations that the conference is being recorded and ask if there are any objections.
 - a. In the event of an objection to the recording of the video conference the Chief Legal Counsel for the Department shall render a decision on the matter.

- b. A failure to complete the required section on the request form and/or a failure to make the announcement of the intention to record the conference shall result in the conference not being recorded.
 - 2. Recording of **non-consensual** inmate video sessions is permissible with the following exceptions:
 - a. With legal counsel
 - b. With Clergy
 - c. Tele-medicine
 - d. Tele-psychiatry
- E. Use of Video Conferencing by an External Agency:
 - 1. Any request for use of a facility video conferencing room and equipment connections by an outside agency shall be forwarded by the System Management Team member or the facility Video Conferencing Coordinator to the Secretary of Corrections for approval.
 - 2. The request shall be submitted on the video request form (Attachment B) at least two (2) weeks prior to the planned usage.
- F. Inmate Video Conferencing sites schedule will be determined by the local facility.
- G. Responsibilities
 - 1. CIO
 - a. Review and approve video conference equipment and service requirements
 - b. Coordinate with DISC for communications services
 - 2. The System Management Team (SMT):
 - a. Designate Video Conferencing Coordinators.
 - b. The number of coordinators and back-up staff shall be determined by the SMT member at each site facility.
 - 3. Video Conferencing Coordinators:
 - a. Staff designated with such responsibilities shall receive training in the operation of video conferencing equipment and the procedures for scheduling.
 - b. Ensure that the video conferencing equipment be operated only by those who have received adequate training associated with video equipment.
 - 4. Enterprise Security Officer:
 - a. Monitor network traffic to ensure that the use of video conference meets network security policies.
 - b. Report any misuse of video conferencing resources to the CIO

VI. Designated Staff Responsibilities

- A. DISC: Responsible for the security and monitoring of the state network.
Information Technology Managers:
 - 1. Maintain network diagrams of all sites and facilities under his/her responsibility
 - 2. Identify information / data production procedures to ensure reliability of the network.
 - 3. Implement network monitoring techniques in coordination with DISC.
- B. Network Administrators:
 - 1. Maintain current listing of network resources
 - 2. Assist the call center in identifying network issues and resolutions
 - 3. Compile monthly status and projects report
- C. Database Server Administrators:
 - 1. Implement techniques to provide redundancy and load balancing.

VII. Trouble Elimination Assistance Management (TEAM)

- A. In the event of an issue, an ad hoc team will be convened to provide assistance to other Information Technology staff.
- B. After all local resources have been exhausted attempting to correct a network problem, the affected facility/office IT staff shall call the Central Office Telecommunication Manager.
- C. The Central Office ESO shall establish an ad hoc team consisting of the following:
 - 1. Technical Support Branch Manager
 - 2. Field Services Support Team Leader
 - 3. Department Network Services Supervisor
 - 4. Eastern Region Team Leader
 - 5. Western Region Team Leader
 - 6. Southern Region Team Leader
 - 7. The affected facility/office IT Staff
 - 8. An at large IT person with specific expertise in the area of the issue.
- D. The team will meet by conference call and will meet as many times as necessary to correct the issue.
- E. If the Central Office ESO cannot be reached, the affected facility/office shall contact the next person in line from the ad hoc team.

- F. If the team cannot determine a correction, the decision shall be made for the affected area's team leader to contact a selected vendor (i.e., Microsoft, etc.).

VIII. Use of Vendor Support

- A. The Kansas Department of Corrections maintains contracts with several vendors who will provide telephonic and on-call support. All requests for vendor-supplied services must be coordinated with the appropriate Central Office support coordinator.

NOTE: The policy and procedures set forth herein are intended to establish directives and guidelines for staff and offenders and those entities who are contractually bound to adhere to them. They are not intended to establish State created liberty interests for employees or offenders, or an independent duty owed by the Department of Corrections to employees, offenders, or third parties. Similarly, those references to the standards of various accrediting entities as may be contained within this document are included solely to manifest the commonality of purpose and direction as shared by the content of the document and the content of the referenced standards. Any such references within this document neither imply accredited status by a departmental facility or organizational unit, nor indicate compliance with the standards so cited. The policy and procedures contained within this document are intended to be compliant with all applicable statutes and/or regulatory requirements of the Federal Government and the state of Kansas. This policy and procedure is not intended to establish or create new constitutional rights or to enlarge or expand upon existing constitutional rights or duties.

REPORTS REQUIRED

Monthly Status Reports

REFERENCES

KSA 21-3755
KSA 75-2949
KSA 75-4709
DISC Standard Operating Procedures 1805.01 & 4206.01
DISC Policy and Procedure Memorandum 5209.00
DISC Policy and Procedure Memorandum 5214.00
Executive Order 02-05
Kansas State Technical Architecture (KSTA)

ATTACHMENTS

Attachment	Title of Attachment	Page Total
A	Cellular Phone/Pager Usage Form	1 page(s)
B	PDA Usage Form	1 page(s)
C	Video Conference Request Form	1 page(s)

To: ALL CELLPHONE USERS

Date:

The following cellular device _____ has been issued
(cell phone sticker #)

to _____. This phone (_ _ _) _ _ _ - _ _ _ _ is to be used for
(name of staff person receiving phone)

business purposes only, unless approved by (appointing authority) for other activity. All non-business calls and texts will be reviewed monthly and may incur charges for usage (amount will be based on *current phone service provider* charges). Do not answer calls or read texts from numbers you do not know. If the phone is damaged or lost, the employee is responsible for notifying their supervisor and/or (other designated staff) to coordinate a replacement.

In using this phone I understand and agree that all electronic content of this phone may be monitored by my employer, the State of Kansas. I further consent to the disclosure to my employer, the State of Kansas, of all information sent and received through this phone including, but not limited to: texts, voice mails, phone number lists, phone number logs and all other data of any sort whatsoever associated with my use of this phone.

(appointing authority name), (appointing authority title)

Signature of staff receiving phone and agreement to terms: _____

PERSONAL DIGITAL ASSISTANT USAGE FORM

Date:

Name of Requestor:

Facility/Department/Division Name:

Agency/Sub-Agency No.:

Purpose of PDA use:

Flash drives are furnished for specific staff use and are not to be used for personal use. Employee misuse of official flash drives may be cause for disciplinary action.

I verify that I have read and fully understand IMPP 05-121, 05-171 and 05-172 and agree to all requirements of the IMPP.

Signature of ESO or designee

Signature of User

VIDEO CONFERENCE REQUEST FORM

		Date:	
Name of Requestor:			
Facility/Department/Division Name:		Agency/Sub-Agency No.:	
Purpose of videoconference facility use:			
Date of videoconference:			
Estimated Beginning Time:		Estimated Ending Time:	
Video Conference Recording:		<input type="checkbox"/> NO <input type="checkbox"/> YES (please check one)	
Reason for video recording:			
Approved/Disapproved - Chief Legal Counsel			
Person who will be responsible for video recording:			
Videoconference Coordinator Signature		System Management Team Signature	
For CO Use:	By (initials)		
DISC Notification (date):			
Actual Ending Time:		Copy to Facility/Department/Division (date)	